We claim:

1. A secure electronic data storage and retrieval system, comprising:

a data repository;

a repository manager for managing storage and retrieval of encrypted electronic data of a depositing computer into and out of the data repository;

an agent program of the depositing computer, accessible to the repository manager whether the depositing computer is online or off-line, the agent program having means to decrypt, on authentication of a requesting computer, the encrypted electronic data of the depositing computer retrieved from the data repository on request of the requesting computer.

2. The system, according to claim 1, where the repository manager is further adapted to digitally sign the encrypted electronic data prior to storage in the data repository, and to forward a copy of the signed encrypted data to the agent program of the depositing computer, and wherein the agent program of the depositing computer is adapted to verify against the signed encrypted data, the retrieved encrypted electronic data following decryption.

3. The system, according to claim 2, wherein the agent program is further adapted to forward the decrypted electronic data to the requesting computer.

4. The system, according to claim 3, wherein the agent program is a secure extension of the depositing computer and is adapted to manage communications between the depositing computer and the repository manager.

5. The system, according to claim 4, further comprising a server having communication links with the repository manager, the depositing computer and the requesting computer, the server housing:

the agent program of the depositing computer;

a second environment comprising a secure extension of the repository manager, said second environment adapted to manage communications to and from other environments on the server with the repository manager; and

at least a third environment comprising a secure extension of the requesting computer, said third environment adapted to manage communications to and from other environments on the server with the requesting computer.

6. The system, according to claim 5, wherein the agent program of the depositing computer comprises means to encrypt and digitally sign electronic data received from the depositing computer, and to forward the encrypted electronic data and signature to the repository manager for storage in the data repository.

7. A process for securely authenticating user access to electronic data stored in a data repository managed by a repository manager unrelated to a source of the electronic data, comprising:

associating an access control list of user authorizations with the electronic data when stored in the data repository;

effecting updates to the access control list from the source of the electronic data;

storing the updated access control list with the electronic data stored in the data repository; storing evidence of the updated access control list at the source of the electronic data and at any user computer to have effected the update; and

verifying accuracy of the updated access control list stored with the electronic data in the data repository with the evidence stored at the source before releasing the electronic data to a requesting authorized user.

8. The process, according to claim 7, wherein the step of effecting updates to the access control list comprises:

identifying a revision level of the updated access control list; and

associating a current time stamp with the updated access control list,

and wherein the step of storing evidence comprises:

creating a token of the revision level and current time stamp; and

storing the token at every user with access to the electronic data in the data repository.

9. The process of claim 8, further comprising:

attaching the token to the updated access control list to form a data structure;

digitally signing the data structure; and

storing the signed data structure with the updated access control list in the data repository and at the source, and wherein the step of verifying accuracy of the updated access control list comprises: verifyingdecrypting the data structure signature at the source; and

comparing the verified data structure with the updated access control list retrieved from the data repository.

10. The process of claim 8, wherein the step of storing evidence further comprises:

digitally signing the token; and

storing the signed token at the source.

11. The process of claim 10, further comprising:

forwarding the digitally signed token to a user authorized by the source to update the access control list; and

on presentation of the digitally signed token by the user authorized to update the access control list,

verifying the token signature at the source; and

comparing the verified token with the revision level and current time stamp associated with the updated access control list retrieved from the data repository.

12. A process for secure storage and retrieval of electronic data in a remote data repository, comprising:

digitally signing the electronic data at source;

encrypting the electronic data at the source;

forwarding the encrypted electronic data to the data repository;

digitally signing the encrypted electronic data at the data repository to produce a deposit receipt;

storing the encrypted electronic data and deposit receipt in the data repository; and

returning a copy of the deposit receipt to the source.

13. The process, according to claim 12, further comprising:

receiving a request from a requesting user, for access to the stored electronic data;

retrieving the encrypted electronic data and forwarding the retrieved data to the source;

verifying the requesting user as authorized to access the electronic data; and

if verified, decrypting the retrieved data.

14. The process, according to claim 13, further comprising:

associating an access control list of user authorizations with the electronic data when stored in the data repository;

effecting updates to the access control list from the source of the electronic data;

storing the updated access control list with the electronic data stored in the data repository; and

storing evidence of the updated access control list at the source and at every user with authorized access to the electronic data in the data repository.

15. The process, according to claim 14, wherein the step of verifying the requesting user as authorized comprises locating the requesting user on the updated access control list.

16. The process, according to claim 15, further comprising the step of verifying accuracy of the updated access control list stored with the electronic data in the data repository with the evidence stored at the source before releasing the electronic data to the requesting user.

17. A computer program product on a computer usable medium for securely authenticating user access to electronic data stored in a data repository managed by a repository manager unrelated to a source of the electronic data, said computer program product comprising:

computer software for associating an access control list of user authorizations with the electronic data when stored in the data repository;

computer software for effecting updates to the access control list from the source of electronic data;

computer software for storing the updated access control list with the electronic data stored in the data repository;

computer software for storing the evidence of the updated access control list at the source of the electronic data and at any user computer to have effected the update; and

computer software for verifying accuracy of the updated access control list stored with the electronic data in the data repository with the evidence stored at the source before releasing the electronic data to a requesting authorized user.

18. The program product of claim 17, wherein the computer software for effecting updates to the access control list comprises:

computer software for identifying a revision level of the updated access control list; and

computer software for associating a current time stamp with the updated access control list, and wherein the step of storing evidence comprises:

computer software for creating a token of the revision level and current time stamp; and

computer software for storing the token at every user with access to the electronic data in the data repository.

19. The program product of claim 18, further comprising:

computer software for attaching the token to the updated access control list to form a data structure;

computer software for digitally signing the data structure; and

computer software for storing the signed data structure with the updated access control list in the data repository and at the source, and wherein the software for verifying accuracy of the updated access control list comprises:

computer software for verifying decrypting the data structure signature at the source; and

computer software for comparing the verified data structure with the updated access control list retrieved from the data repository.

20. The program product of claim 18, wherein the computer software for storing evidence further comprises:

computer software for digitally signing the token; and

computer software for storing the signed token at the source.

21. The program product of claim 20, further comprising:

computer software for forwarding the digitally signed token to a user authorized by the source to update the access control list, and

on presentation of the digitally signed token by the user authorized to update the access control list,

verifying the token signature at the source; and

comparing the verified token with the revision level and current time stamp associated with the updated access control list retrieved from the data repository.

22. A computer program product on a computer for secure storage and retrieval of electronic data in a remote data repository, comprising:

computer software for digitally signing the electronic data at source;

computer software for encrypting the electronic data at the source;

computer software for forwarding the encrypted electronic data to the data repository;

computer software for storing the encrypted electronic data and deposit receipt in the data repository; and

computer software for returning a copy of the deposit receipt to the source.

23. The program product according to claim 22, further comprising:

computer software for receiving a request from a requesting user, for access to the stored electronic data;

computer software for retrieving the encrypted electronic data and forwarding the retrieved data the source;

computer software for verifying the requesting user as authorized to access the electronic data; and

computer software product for decrypting the retrieved data when verified.

24. The computer program product according to claim 18, further comprising:

computer software for associating an access control list of user authorizations with the electronic data when stored in the data repository;

computer software for effecting updates to the access control list from the source of the electronic data;

computer software for storing the updated access control list with the electronic data stored in the data repository; and

computer software for storing evidence of the updated access control list at the source and at every user with authorized access to the electronic data in the data repository.

25. The computer program product according to claim 24, wherein the computer software for verifying the requesting user as authorized comprises computer software for locating the requesting user on the updated access control list.

26. The computer program product according to claim 25, further comprising computer software for verifying accuracy of the updated access control list stored with the electronic data in the data repository with the evidence stored at the source before releasing the electronic data to the requesting user.